UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,751	02/23/2004	Nicolas Popp	12832/100002	6185

20350 7590 08/01/2008

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
08/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/782,751	POPP, NICOLAS	
	Examiner	Art Unit	
	MICHAEL J. SIMITOSKI	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *3-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 April 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/14/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response and IDS of 4/14/2008 were received and considered.

2. Claims 3-14 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 3-4 have been considered but are moot in view of the new ground(s) of rejection.

4. Applicant's response cancels claims 1-2 and adds new claims 3-14. The application of the newly-cited Dutta reference, in combination with the other applied references, is given below.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 3, 5 & 7-8 are rejected under 35 U.S.C. 102(a)/102(e) as being anticipated by U.S. Patent Application Publication 2003/0093667 to Dutta et al. (**Dutta**).

Regarding claim 3, Dutta discloses a method of provisioning a first token (PTD, ¶57) having a first secret (private key, ¶57), comprising sending a request for a certificate (redemption

step requests RVO, Fig. 4, step C), receiving a certificate (Take_ticket) that contains a second secret (RVO, ¶63) encrypted with a public key of the token (RVO encrypting with TPD_PuK, Fig. 4, step D), the second secret (RVO) distinct from the first secret (RVO is not the same as the private key of the PTD), decrypting the second secret with a private key of the token (decryption is not explicitly shown, however, it is inherent as the RVO is used by the PTD to generate the RVT/pseudo-random sequence, ¶63 & ¶67, and the RVO is received in encrypted form, Fig. 4, step D & ¶67) and generating a one time password (RVT) based on the second secret (generating the RVT/pseudo-random sequence based on the RVO received, ¶63 & ¶¶75-76).

Regarding claim 5, Dutta discloses wherein the second secret (RVO) is a symmetric cryptographic key (value used to generate a password/RVT, ¶63). It is noted that a symmetric cryptographic key is a data value.

Regarding claim 7, Dutta discloses wherein the one time password (RVT) based on the second secret (RVO) is further based on a signal from a clock (S/P generator also generates RVT based on a clock value, ¶67).

Regarding claim 8, Dutta discloses wherein the one time password based on the second secret is further based on a counter value (S/P generator also generates RVT based on a clock value, which is a form of counter, ¶67).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dutta**, as applied to claim 1 above, in view of U.S. Patent Application Publication 2002/0131592 to Hinnant et al. (**Hinnant**).

Regarding claim 4, Dutta discloses a system where a personal device, such as a PDA or computer, receives a rapid verification object. The RVO is used as a seed, possibly with other information, to generate and RVT/pseudo-random sequence which is sent to and verified at another device (rapid verification system). Dutta lacks subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret. However, Hinnant teaches that it is well known to generate keys using a pseudorandom number generate that is based on a seed (¶8) and that it is also known that, because the seed can be recovered/compromised (¶9), it is known to update the seed to maintain the security of the pseudorandom sequence (¶11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dutta's PDT to received updated seeds (RVO) and thus generate one time passwords based on a first secret (received seed), in a manner as described above, and to received a second secret (updated seed/new RVO), after which generation of one time passwords based on the first secret (old seed) is discontinued. One of ordinary skill in the art would have been motivated to perform such a modification to avoid problems with the RVO being recovered by an attacker by updating the seed/RVO to maintain the security of the system, as taught by Hinnant.

9. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dutta**, as applied to claim 1 above, in further view of "Strong Enterprise User Authentication: RSA ACE/Server" by RSA Security (**RSA**).

Regarding claim 6, Dutta lacks wherein the one time password (RVT, also called the pseudo random sequence, ¶67) based on the second secret is further based on a personal identification number. However, RSA teaches that the addition of a second factor (PIN) is a stronger form of authentication (p. 3, §II, ¶1), where a token code is read from the token and entered along with a PIN, where the software hashes the values and submits them for authentication (p. 4, ¶¶1-2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dutta to allow a user to input a PIN to be combined with the RVO/seed generated to generate a one time password. One of ordinary skill in the art would have been motivated to perform such a modification to gain on of the benefits of a second form of authentication, such as increased certainty of authenticity, as taught by RSA.

10. Claims 9, 11 & 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Dutta** in view of U.S. Patent 7,197,072 to Hsu et al. (**Hsu**).

Regarding claim 9, Dutta discloses a token (PTD, Fig. 1, #16) for generating one time passwords comprising a processor (PTD, Fig. 3, #16, including security element, Fig. 1, #20, Fig. 3, #20 and functional element, Fig. 3, #40) and a memory coupled to the processor (Fig. 3, #52 & Fig. 3, #62), the memory storing a first secret (stores PTKPrK, Fig. 3, #62) and executing the processor to send a message that includes a request for a certificate (redemption step requests RVO, Fig. 4, step C), receive a certificate (Take_ticket) that contains a second secret (RVO)

encrypting with a public key of the token (RVO encrypting with TPD_PuK, Fig. 4, step D), decrypt the second secret with a private key of the token (decryption is not explicitly shown, however, it is inherent as the RVO is used by the PTD to generate the RVT/pseudo-random sequence, ¶63 & ¶67, and the RVO is received in encrypted form, Fig. 4, step D & ¶67), store the second secret in memory (S/P generator stores the RVO, which contains a seed, for generation of a pattern/sequence, Fig. 3, #64, ¶46 & ¶63) and generate a one time password (RVT) based on the second secret (generating the RVT/pseudo-random sequence based on the RVO received, ¶63 & ¶¶75-76). Dutta discloses in ¶68 that the security element comprises a program (computer instructions) to perform its actions, but lacks explicitly that the functional element processor includes token instructions for execution on the processor to perform the functions of the functional element. However, Hsu teaches where a processor can be an application specific processor or a general-purpose computer executing software instructions (col. 4, lines 19-26) where the general-purpose hardware with software solution provides more upgradeability and lower cost than dedicated hardware (col. 16, line 16 – col. 17, line 5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dutta to explicitly include token instructions adapted to be executed by the processor to perform the sending, receiving, decrypting, storing and generating steps. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefits of upgradeability and lower cots, as taught by Hsu.

Regarding claim 11, Dutta discloses wherein the second secret (RVO) is a symmetric cryptographic key (value used to generate a password/RVT, ¶63). It is noted that a symmetric cryptographic key is a data value.

Regarding claim 13, Dutta discloses wherein the one time password based on the second secret is further based on a signal from a clock (S/P generator also generates RVT based on a clock value, ¶67).

Regarding claim 14, Dutta discloses wherein the one time password based on the second secret is further based on a counter value (S/P generator also generates RVT based on a clock value, which is a form of counter, ¶67).

11. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dutta** and **Hsu**, as applied to claim 9 above, in further view of **Hinnant**.

Regarding claim 10, Dutta discloses a system where a personal device, such as a PDA or computer, receives a rapid verification object. The RVO is used as a seed, possibly with other information, to generate and RVT/pseudo-random sequence which is sent to and verified at another device (rapid verification system). Dutta lacks subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret. However, Hinnant teaches that it is well known to generate keys using a pseudorandom number generate that is based on a seed (¶8) and that it is also known that, because the seed can be recovered/compromised (¶9), it is known to update the seed to maintain the security of the pseudorandom sequence (¶11). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dutta's PDT to received updated seeds (RVO) and thus generate one time passwords based on a first secret (received seed), in a manner as described above, and to received a second secret (updated seed/new RVO), after which generation of one time passwords based on the first secret (old seed) is discontinued. One

of ordinary skill in the art would have been motivated to perform such a modification to avoid problems with the RVO being recovered by an attacker by updating the seed/RVO to maintain the security of the system, as taught by Hinnant.

12. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Dutta** and **Hsu**, as applied to claim 9 above, in further view of **RSA**.

Regarding claim 12, Dutta lacks wherein the one time password (RVT, also called the pseudo random sequence, ¶67) based on the second secret is further based on a personal identification number. However, RSA teaches that the addition of a second factor (PIN) is a stronger form of authentication (p. 3, §II, ¶1), where a token code is read from the token and entered along with a PIN, where the software hashes the values and submits them for authentication (p. 4, ¶¶1-2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Dutta to allow a user to input a PIN to a to the PTD (¶29) to be combined with the RVO/seed generated to generate a one time password. One of ordinary skill in the art would have been motivated to perform such a modification to gain on of the benefits of a second form of authentication, such as increased certainty of authenticity, as taught by RSA.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL J. SIMITOSKI whose telephone number is (571)272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

July 23, 2008
/Michael J Simitoski/
Primary Examiner, Art Unit 2134